The European Federation of Loss Adjusting Experts

FUEDÍ

# Professional, impartial, independent. >

CÂMARA NACIONAL DE PERITOS REGULADORES

fuedi.eu

# Cyber Risks & Cyber Crime
# Lisboa

*26. October 2018*
*Mark Vos, B Eng, FCILA, FUEDI-ELAE*
*FUEDI workgroup Cyber*
*markvos@crawco.nl*

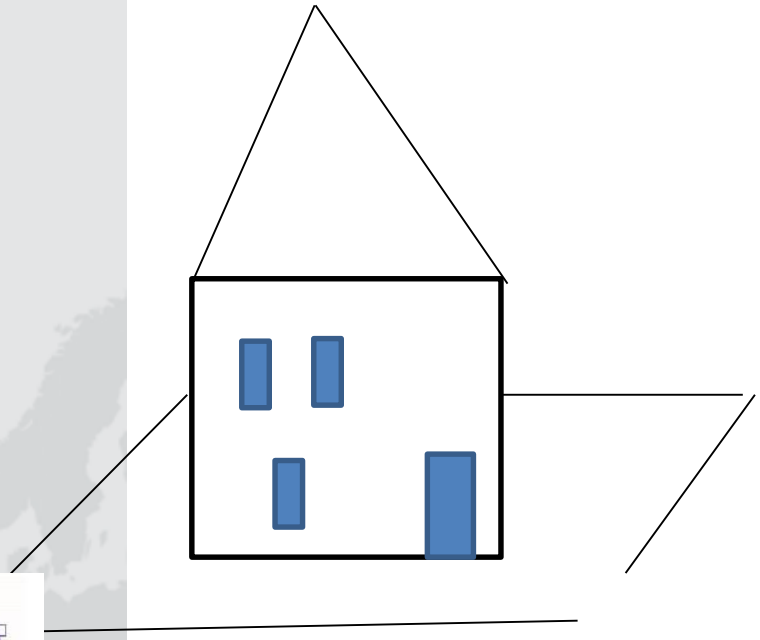
# Cyber risk


- Loss of control
  - Hardware
  - Operating System etc
  - Application software
  - Data  and, or Data integrity

- Situation of Risk
  - At Insured address
  - In EU or outside EU
    - Insured's controlled location
    - Cloud


CÂMARA NACIONAL DE PERITOS REGULADORES

# Property Risk metaphore
# Basic risk prevention layers



House = Computer
Ground floor = Operating System + access door
First floor = Application software
Windows = software patch, updates at either level
Front door = Access management ; ID + Password
Jewelry = Valuable Data
High value → safe = Double token access
Precious value in safe = Encryption of data
Fence around house = Firewall
Camera's around house to spot behavior = SIEM Security Information and Event Management
Alternative access doors = Web shop, etc communication via other gates

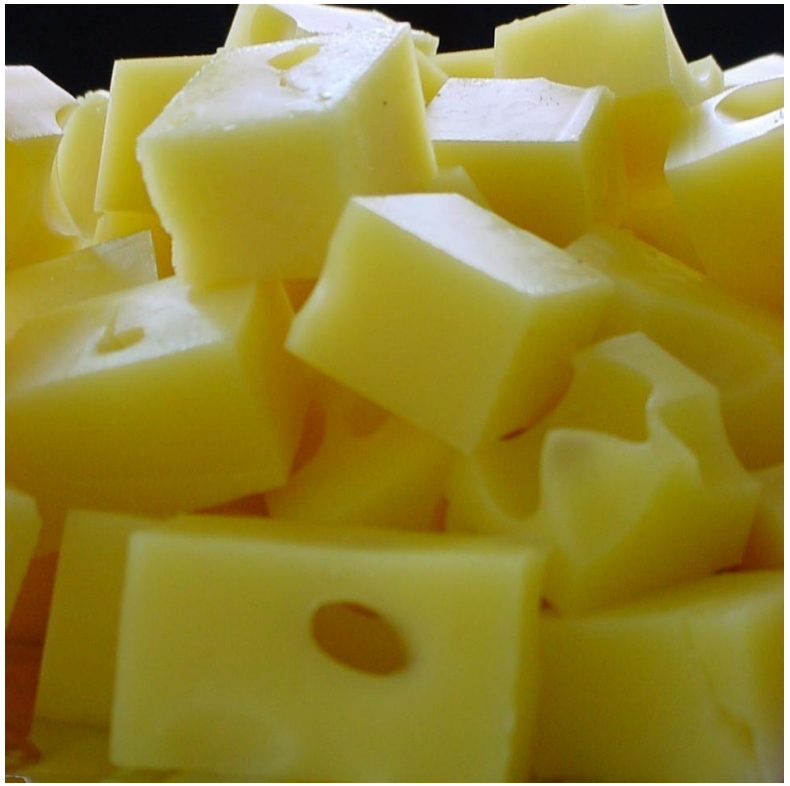
# Cause & Forensic Investigation

- Computer is also used for communication
- Open gates to outside world
- Risks = access point of communication
  - Email
  - Web applications
  - Internet
  - LAN – WAN inter-company
  - USB – Flash disks
- Defence & Security at each risk levels
- Quality of IT suppliers & System Updates
- 5 to 6,000 new virus per day

# Security incident and its conflict

- Fire once every 10 years
- Cyber once every 10 mill second
- Write off period of computer networks
- Write off period of computer supported machines like laboratory testers
- New security software versus aged systems, which cannot be protected at AAA level.

# How structured is your organisation ?



# 10 Steps to Cyber Security

- 1. Secure Configuration
- 2. Network Security
- 3. Malware Protection
- 4. Removable Media Controls

- 5. Managing User Privileges
- 6. User Education Awareness
- 7. Home & Mobile Working

Contractors & Consultants

The World

8. Information Risk Management Regime
9. Monitoring
10. Incident Management

# Business Continuity, Disaster Recovery

- Why companies need to plan for a cyber event
- The crisis nature of a cyber event
- The importance of appointing a single coordinator
  able to bring in specialists when required.

# Business Continuity Plan, Role Responsibilities

- 1: In case of a breach legal council needed?
  - Do we have legal knowledge in-house to respond at all levels
- 2: Is IT and Crisis management organisation ready ?
  - To defend against hack?
  - Every back-up virus free?
- 3: Mandatory publication interests of consumers?
  - Loss of image , Public Relation exposure, Press releases < 24 hrs.
- 4: Who and how do you inform authorities in your country
  - AND all countries of your affected consumers?
- 5: Breach of Data Protection Act.
  - Who and how will you inform x000 of consumers?
- 6: What is time frame of response < 24 hrs to authorities?
  - Are you in control or the National Cyber Security Police in control.
- 7: Who is coordinating this internally?
  - Holidays / Business trips of key persons.

# Cyber risk and insurance

- Cyber clause in Property Policy
  - - Property risk per location
  - - Multiple locations of IT system
    - Data centre,
    - Servers,
    - Work stations,
    - Cloud,
    - IP6 – Internet of Things
  - Conclusion Property policy with Virus clause is not ideal.

# Cyber risk in other policies

- Liability risk ,
  - Material damage,
  - GDPR – non-material damage
- Construction All Risk, EAR,
  - New equipment with virus / hack software included,
  - (hot) Testing with cyber risk,
- Maintenance & Warranty ,
  - Leaving virus behind,
  - Wind and Solar power installations,
  - Internet of Things , IP6
- Marine & Transportation,
  - Hacking at ports and theft of cargo.

# Cyber & Insurance products

- Direct cover of (non-)material damage and financial loss
- Cover of assistance to resolve the consequences of losing control of hardware, software and data integrity.
- Direct support via
  - a legal route mainly data privacy breach
  - a loss adjuster route acting as crisis manager

# How does a cyber loss look like (1)

- Web shop with copied consumers
  - GDPR risk is consumer related
    - 43 different nationalities
  - Old web site software new under construction
- Ukraine Petya virus
  - Isolated network of subsidiary but linked via financial reporting
- Phishing telecom email with virus
  - Network down, but no defence for laboratory environment
  - Lab equipment with XP computers
  - Need mirror data exchange to create defence at high standard anti virus software level

# How does a cyber loss look like (2)

- Marketing email
  - CC of clients instead of BCC
  - GDPR attack / Risk of personal identity
    - List of consumers of courier
    - List of medical users
- Phishing mail
  - Subsidiary versus Parent company
  - Budget 2019 versus budget 2017
- Password disclosure at Forum
  - Company password identical at Open Source Forum,
  - Access of Contractor to Employers project data base
  - Work outside office hours,???

# How does a cyber loss look like (3)

- Redemption action
  - Too many respondents
  - Software bug or hack

Conclusion:

Small companies do not have different risks, which are necessarily smaller.

# Emerging risks & Value chain

- Material damage and non-material damage principle to be embraced
- Non-material damage, professional indemnity, and product liability
  - System down, but which system
  - Data in (de-)centralized world
  - Blockchain in decentralized world
  - Digital revolution like remote surgery, 3D printing
- Non-material damage BI
- Internet of Things in the value chain
  - Outsourced control of assets
  - Supply risk
  - Vendor risk
  - Business Interruption risk outside the location
  - Is 24 month indemnity period too long or too short

# Cyber Insurance

**Cyber Insurance**
**and**
**Cyber loss adjusters.**

**THANK YOU**

**www.fuedi.eu**